

AO 91 (Rev. 11/11) Criminal Complaint

## UNITED STATES DISTRICT COURT

for the  
Northern District of New York

UNITED STATES OF AMERICA

v.

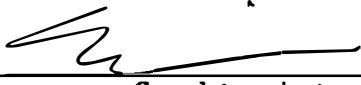
Case No. 3:20-MJ-541 (ML)

NICOLAE FLORIN MARES a/k/a  
ZOLTAN BALOGH

Defendant(s)

## CRIMINAL COMPLAINT

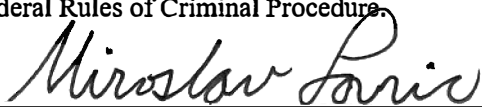
I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of September, 2019 in the county of Delaware in the Northern District of New York the  
defendant(s) violated:*Code Section*  
**Title 18, United States Code, Section  
1344***Offense Description*  
**Bank Fraud**This criminal complaint is based on these facts:  
**See Attached Affidavit**☒ Continued on the attached sheet.  
Complainant's signature

Stephen W. Vizvary, Special Agent, FBI

Printed name and title

Attested to by the affiant in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

Date: October 27, 2020  
Judge's signatureCity and State: Binghamton, New York

Hon. Miroslav Lovric, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR ISSUANCE OF CRIMINAL  
COMPLAINT AND ARREST WARRANT**

STEPHEN W.VIZVARY, being duly sworn, deposes and states:

**INTRODUCTION**

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and I am empowered by law to investigate and to make arrests for criminal offenses enumerated in Section 2516 of Title 18 of the United States Code. As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7).

2. I have been employed as a Special Agent of the FBI since May 2004. I am currently assigned to the Binghamton Resident Agency in Binghamton, New York where I conduct investigations into various types of computer criminal activity, to include financially motivated computer intrusions, state sponsored computer intrusions, and cyber terrorism. I am familiar with and have received extensive training regarding the use of computer technology to conduct criminal activity. I have attained computer security credentials from the Global Information Assurance Certification (GIAC) as both a Certified Intrusion Analyst as well as a Certified Forensic Analyst.

3. I submit this Affidavit in support of an application for the issuance of a criminal complaint and arrest warrant authorizing the arrest of **NICOLAE FLORIN MARES AKA "ZOLTAN BALOGH."** This Affidavit sets forth facts and evidence demonstrating there is probable cause to believe violations of federal law, including but not limited to, Title 18, United States Code, Section 1344 (Bank Fraud) have been committed by **NICOLAE FLORIN MARES AKA "ZOLTAN BALOGH."**

4. The statements and facts set forth in this Affidavit are based in significant part on my training and experience as a Special Agent with the FBI, information obtained from other law

enforcement officials, federal and state records, victim interviews, and surveillance photos and videos.

5. Since this Affidavit is being submitted for the limited purposes of securing a criminal complaint and arrest warrant, your Affiant has not included every fact known to me concerning this investigation. Instead, your Affiant has set forth only facts I believe are necessary to establish the foundation for securing a criminal complaint and arrest warrant.

#### **BACKGROUND OF THE INVESTIGATION**

6. On September 3, 2019, the Walton Police Department in Walton, New York contacted the New York State Police (NYSP) requesting NYSP assistance with a fraud case involving several Sidney Federal Credit Union (SFCU) customer accounts wherein United States currency had been removed from these accounts without authorization. The United States currency had been removed in the form of Automated Teller Machines (ATM) cash withdrawals totaling a potential loss of \$100,000. On the same date, NYSP interviewed SFCU personnel. After an internal review, SFCU personnel advised NYSP they believed a total of five ATMs may have been compromised during the fraudulent activity.

7. On September 4, 2019, NYSP interviewed the branch manager for SFCU in Walton, New York. The SFCU manager stated that on Saturday August 31, 2019, she had been notified by some of her staff members that SFCU account holders had been posting on social media about fraudulent ATM transactions at SFCU. The SFCU branch manager came into the Walton SFCU on the evening of August 31, 2019, to run a test for skimmers<sup>1</sup> on the Walton ATM, which produced negative results. The SFCU branch manager called Diebold, the company that services

---

<sup>1</sup> A skimmer is a device which is installed on an ATM or other comparable electronic device and alters the functionality of an electronic device to record customers' ATM card numbers and access or pin codes.

SFCU ATMs; Diebold sent a technician to the Walton branch location on September 1, 2019, and ran additional tests, printing a status log which showed numerous events of fraud devices being detected and removed on the ATM between July 12, 2019, and August 28, 2019. Based upon this information, as well as your affiant's training and experience in investigating these types of criminal activity, your affiant believes these fraud device detection and removal alerts indicate attempts by unknown subject(s) to tamper with, install, or otherwise alter the functionality and operation of the ATM machine to record customers' ATM card numbers and access or pin codes without the customer's knowledge.

8. SFCU obtained surveillance camera footage from the Walton, New York and Oneonta, New York SFCU<sup>2</sup> during the time in which the fraudulent activity was believed to have occurred. On August 7, 2019, surveillance video depicts an individual tampering with the ATM at the Oneonta SFCU. Specifically, the surveillance video shows the individual removing the front cover of the ATM. A person with the same physical characteristics and wearing what appears to be the same hat, as well as the same make and model vehicle parked in front of the Oneonta SFCU ATM, was also observed at the Walton SFCU ATM on August 14, 2019. After reviewing the video surveillance footage, your affiant believes that the individual from the Oneonta SFCU ATM on August 7, 2019, and the Walton SFCU ATM from August 14, 2019, are the same individual.

9. On September 4, 2019, SFCU advised NYSP a total of 523 SFCU customer accounts had been reported to have fraudulent activity over the 2019 Labor Day Weekend through two compromised ATMs, (located at the Walton and Oneonta branches), with the total approximate loss of \$200,000. To mitigate future losses, SFCU blocked and ultimately re-issued

---

<sup>2</sup> SFCU employees determined that the fraudulent transactions originated from these two SFCU branches.

new ATM cards for approximately 1,500 SFCU customer accounts that were potentially compromised.

10. On September 4, 2019, SFCU advised law enforcement they had been contacted by West Virginia Pulp and Paper Company (WEPCO) Federal Credit Union in the state of Maryland where some of the fraudulent SFCU ATM card numbers were used to make cash withdrawals.

11. On September 5, 2019, the NYSP contacted the Garrett County Sheriff's Office (GCSO) in Maryland. GCSO advised NYSP they had been contacted by WEPCO Federal Credit Unit in Western Maryland after WEPCO observed fraudulent ATM activity involving ATM cards that were associated with SFCU accounts in Sidney, New York. GCSO reported to the NYSP that cash-outs<sup>3</sup> of SFCU accounts had occurred in the Maryland towns of Levale, Bloomington, and Oakland for losses of approximately \$21,900, \$31,200, and less than \$1,000 respectively. GCSO also advised there were cash-outs of SFCU accounts at two WEPCO West Virginia ATM locations in the towns of Keyser and Kingwood for the approximate amounts of \$36,000 and \$11,300 respectively.

12. On September 4, 2019, as part of the GCSO investigation into the ATM fraud, a meeting was held between GCSO and WEPCO FCU. WEPCO FCU advised GCSO that during the withdrawal of approximately \$31,200 from SFCU customer accounts by unknown subjects at the Bloomington, Maryland ATM, four (4) receipts and \$60.00 were left in and around the ATM vestibule. WEPCO advised GCSO the \$60.00 was placed back into the bank teller drawers, however, the four ATM receipts were recovered and preserved for law enforcement. As part of their investigation, members of the GCSO collected the receipts from WEPCO and transported

---

<sup>3</sup> Cash-outs are the unauthorized cash withdrawals via ATM from the accounts which were previously compromised using skimmers.

them to the GCSO Evidence Lab to be packaged and sent to the Maryland State Police Crime Lab for various forms of forensic examination.

13. On November 14, 2019, the Maryland State Police Crime Lab (MSPCL) provided GCSO a report containing their findings which your affiant has received and reviewed. Based upon the findings of the Maryland State Police Crime Lab, eight (8) latent fingerprints and one (1) latent palm print were recovered from (3) three of the (4) four ATM receipts collected by GCSO on September 2, 2019. The examination revealed that two (2) of the individual latent fingerprints were recovered from a WEPCO ATM receipt with an account number ending in 6608, which showed a transaction time of 5:48 PM on September 2, 2019. These prints were submitted in AFIS which resulted in a positive match to the known fingerprints of an individual identified as ZOLTAN BALOGH with an FBI Number of EPNVRPCPV.<sup>4</sup> MSPCL then manually compared the fingerprints they collected to those returned from AFIS as belonging to BALOGH and confirmed the fingerprints were identical. WEPCO later advised GCSO they had no record of BALOGH being a member of their financial institution.

14. Your affiant has reviewed surveillance video of the Bloomington WEPCO ATM for the time at which the ATM receipt for account ending in 6608 was generated. This video showed that the subject, who is visually similar to NICOLAE MARES (aka ZOLTAN BALOGH), is at the ATM retrieving both money and receipts from the ATM at 5:48 PM on September 2, 2019. Furthermore, the subject is the only individual in the ATM vestibule between 5:44 PM and

---

<sup>4</sup> A review of BALOGH's criminal history reveals that BALOGH is an alias of NICOLAE MARES, with the same FBI number. As will be further detailed below, a review of booking photographs from his arrests under both names reveals photographs of the same person. MARES admitted in June 2020 that his actual name was NICOLAE MARES.

6:30 PM on September 2, 2019, where he appears to be making continuous transactions at the ATM during this time frame.

15. On September 3, 2020, your affiant reviewed the criminal history for ZOLTAN BALOGH with FBI Number of EPNVRPCPV. It was learned that ZOLTAN BALOGH is an alias for NICOLAE FLORIN MARES. Furthermore, your affiant learned MARES, using the alias ZOLTAN BALOGH, was arrested by the New York Police Department (NYPD) on October 15, 2018, and charged with Grand Larceny related to a pickpocketing incident. Additionally, MARES, was arrested by NYPD on August 28, 2020, for a December 7, 2018, skimming incident in which he was working in concert with another individual to install a deep insert skimmer<sup>5</sup> and a false pinhole camera at an ATM machine located inside of Dime Bank located at 45-14 46<sup>th</sup> Street, Long Island City, New York. A review of the criminal history also showed MARES was not yet charged for the withdrawals of currency from SFCU customer accounts at WEPCO ATMs in Maryland, discussed above.

16. On September 3, 2020, I reviewed an investigation report from the Hanover County Sheriff's Office dated June 3, 2020, in which MARES was arrested in Mechanicsville, Virginia for credit card theft and fraud. During the search of his person MARES was found with U.S. currency and a stack of gift cards from a grocery store chain. Each card had a 4-digit number written on them. During the incident MARES made post *Miranda* statements in which he told Hanover County Sheriff's Office investigators, in part, that his name was NICOLAE MARES and

---

<sup>5</sup> Insert skimming devices are made to fit tightly and invisibly inside an ATM's card acceptance slot. These differ from traditional overlay skimmers which are designed to be placed over the top of a card acceptance slot of an ATM. A pinhole camera is often placed above or on the side of the ATM to video capture the PIN number entered by the legitimate account holder during an ATM transaction. These PIN numbers are later associated with the customer data obtained from the skimming device to provide all necessary information needed to withdraw funds from an ATM without the knowledge or consent of the authorized user.

that he worked for a man in Washington, DC and traveled around skimming information from ATM machines. MARES stated he would receive 20-25 percent of each transaction. MARES said he spent most of his money on “crack” cocaine and was in debt.

17. In addition to the biometric information placing MARES at the Bloomington WEPCO ATM on September 2, 2019, your affiant has obtained and compared the arrest/booking photographs of MARES taken during the August 28, 2020, arrest by the NYPD under the name NICOLAE MARES, the arrest booking photographs taken during the October 15, 2018, arrest by NYPD under the name ZOLTAN BALOGH, and the photograph obtained from ATM surveillance footage from the Bloomington, Maryland WEPCO ATM on September 2, 2019. Upon review of those booking photographs for ZOLTAN BALOGH, NICOLAE MARES and the surveillance footage from the Bloomington, Maryland WEPCO ATM on September 2, 2019, your affiant believes they are all the same person whose true name is NICOLAE MARES. Therefore, based upon your affiant’s review, as well as review by the other investigators from the NYSP who have participated in this investigation, your affiant believes MARES is an individual withdrawing SFCU funds from the WEPCO ATM in Bloomington, Maryland on September 2, 2019, as detailed above.<sup>6</sup>

18. Therefore, your affiant and the other investigators participating in this investigation believe MARES fraudulently obtained compromised financial information under the custody or control of Sidney Federal Credit Union, a financial institution headquartered in Sidney, New York, which was obtained from skimmers placed on Sidney Federal Credit Union ATMs in the Northern District of New York between July and August of 2019, and utilized the compromised financial

---

<sup>6</sup> Surveillance video reflects at least one other unidentified potential co-conspirator who was also responsible for withdrawing funds from SFCU funds from WEPCO ATM on September 2, 2019.



information from Sidney Federal Credit Union in order to withdraw differing sums of United States currency from other financial institutions located outside the Northern District of New York, to include but not limited to, the WEPCO Federal Credit Union in Bloomington, Maryland on September 2, 2019.

**CONCLUSION**

19. WHEREFORE, your affiant submits there is sufficient probable cause to believe **NICOLAE FLORIN MARES, AKA "ZOLTAN BALOGH,"** on or about September 3, 2019, committed bank fraud, in violation of Title 18, United States Code, Section 1344, by fraudulently obtaining moneys under the custody or control of Sidney Federal Credit Union, a financial institution headquartered in Sidney, New York, which is located in the jurisdiction of the Northern District of New York. Accordingly, your affiant respectfully requests this Court issue a criminal complaint and arrest warrant for **NICOLAE FLORIN MARES AKA "ZOLTAN BALOGH."**

ATTESTED TO BY THE AFFIANT



Stephen W. Vizvary  
Special Agent  
Federal Bureau of Investigation

I, the Honorable Miroslav Lovric, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on October 27, 2020 in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure



HONORABLE MIROSLAV LOVRIC  
UNITED STATES MAGISTRATE JUDGE